

REMARKS

Applicants thank the Examiner for the Examiner's comments, which have greatly assisted Applicants in responding.

5

Claims 1-30 are pending in the present application. Claims 1, 7, 8, 11, 17, 28, and 29 have been amended to provide further clarification. No new matter has been entered. Applicants respectfully request reconsideration and allowance of all claims in light of the following arguments.

10

Specification

The abstract of the disclosure was objected to because the text at lines 1-3 is not a proper heading. Applicants submit that the text at lines 1-3 recites the title of the invention and that the heading ABSTRACT is proper. Applicants respectfully believe that the Abstract of the Disclosure complies with MPEP 608.01(b) and request withdrawal of the objection to the Specification.

15

Claim Objections

20

Claims 11-13 and 19-20 were objected to for failing to conform to standard claim numbering practice. Applicants submit that Claims 11-13, and 19-20, as preliminarily amended, comply with standard claim numbering practice and respectfully request withdrawal of the objections to the Claims.

25

Claim Rejections Under 35 USC § 112

Claims 1-16 were rejected under 35 USC § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention.

30

Claims 1, 7, 8, and 11 have been amended for further clarification and to address the Examiner's rejections. Applicants respectfully request withdrawal of the rejections and allowance of the Claims.

5

Claim Rejections Under 35 USC § 102

Claims 1-7, 14, 16-17, 19, 23, 25-28, and 30 were rejected under 35 USC 102(e) as being anticipated by U.S. Patent No. 5,850,443 to Van Oorschot et al. (hereinafter "Van Oorschot"). Applicants respectfully submit that Van Oorschot
10 fails to teach, suggest, or render obvious the present invention as claimed.

Claims 1, 7, 17, 28 have been amended. No new matter has been entered. Support for the amendments can be found, for example, at page 5, first paragraph, at page 6, second paragraph, and page 7, first paragraph of the
15 English translation of the application. Further support can also be found, for example, at page 19, second paragraph.

Independent Claims 1, and 28, as amended recite, *inter alia*, the step of encrypting a first section of the payload data, while a second section of the
20 payload data remains unencrypted, the step of processing the unencrypted second section for obtaining the information characterizing the unencrypted second section, and the step of linking the payload data key with the obtained information by means of an invertible logic linkage to obtain a basic value. Independent Claim 17, as amended, recites a method for decrypting an
25 encrypted payload data stream comprising a header and a payload data block containing a first section having encrypted payload data and a second section having unencrypted payload data, the method comprising, *inter alia*, the step of processing the unencrypted second section of said payload data using the processing method used when encrypting to deduce information characterizing
30 the unencrypted second section.

Looking at the cited references, as outlined in Figure 3 and at col. 6, lines 37-65, Van Oorschot discloses that a message is encrypted using a symmetric

encryption. The symmetric key K' used for the symmetric encryption is encrypted using a public key. Then, the public key, as well as the encrypted symmetric key K' are combined to obtain the X field. Then, a hash value of the data stream X is formed. Then the symmetric key is XORed with the value $h_{40}(X)$, which represents the 40 most significant bits of the hash result. The X field is entered into the final data stream, which, in addition, includes the encrypted message as well as A's header field and B's header field. The header field for A or B is generated by public-key encryption of the levelled key, which is the output of the levelling function block in Figure 3.

Van Oorschot fails to teach or suggest the above limitations recited in Claims 1, 17, and 28, as amended. In Van Oorschot, the whole message is encrypted to obtain the encrypted message. Contrary thereto, Claims 1, 17, and 28 recite that only the first section of the payload data is encrypted, while the second section of the payload data remains unencrypted. In Van Oorschot, the input into the levelling function is processed from the X-field using the hash function $h(X)$ as outlined at col. 6, line 50. The X-field does not include any information based on the message. Contrary thereto, Claims 1, 17, and 28 recite processing of the unencrypted second section to deduce information characterizing the unencrypted second section of the payload data.

Thus, Applicants respectfully submit that Claims 1, 17, and 28, as amended, are distinguishable over Van Oorschot and should be allowed. Claims 2-7, 14, 16, 19, 23, 25-27, and 30, dependent directly or indirectly from Claims 1, 17, and 28, respectively, are also distinguishable over Van Oorschot and should also be allowed at least for the same reasons as stated above. As a result, Applicants respectfully request withdrawal of the rejections and allowance of the Claims.

Claim Rejections Under 35 USC § 103

Claims 8, 11, 12, 18, and 20-21 were rejected under 35 USC 103(a) as being unpatentable over Van Oorschot in view of US Patent No. 5,200,999 to Matyas (hereinafter "Matyas"). Applicants respectfully submit that Van Oorschot and

Matyas, taken alone or in combination, fail to teach, suggest or render obvious the present invention as claimed.

5 Claims 8, 11, 12, 18, 20-21 depend directly or indirectly from allowable Claims 1 and 17, respectively. Van Oorschot fails to teach or suggest the step of encrypting a first section of the payload data, while a second section of the payload data remains unencrypted, the step of processing the unencrypted second section for obtaining the information characterizing the unencrypted second section, and the step of linking the payload data key with the obtained
10 information by means of an invertible logic linkage to obtain a basic value, as claimed in Claims 1, as amended. Van Oorschot also fails to teach or suggest a method for decrypting an encrypted payload data stream comprising a header and a payload data block containing a first section having encrypted payload data and a second section having unencrypted payload data, the method
15 comprising, *inter alia*, the step of processing the unencrypted second section of said payload data using the processing method used when encrypting to deduce information characterizing the unencrypted second section, as claimed in Claim 17, as amended.

20 Matyas does not remedy any of the deficiencies of Van Oorschot. Matyas, taken alone or in combination with Van Oorschot, fails to teach or suggest the above limitations of Claims 1 and 17, as amended.

25 Thus, Applicants respectfully submit that Claims 8, 11, 12, 18, and 20-21 are distinguishable over Van Oorschot and Matyas, taken alone or in combination, and should be allowed. As a result, Applicants respectfully request withdrawal of the rejections and allowance of the Claims.

30 Claim 9 was rejected under 35 USC 103(a) as being unpatentable over Van Oorschot and Matyas and further in view of US Patent No. 5,710,814 to Klemba et al. (hereinafter "Klemba"). Applicants respectfully submit that Van Oorschot,

Matyas, and Klemba, taken alone or in combination, fail to teach, suggest or render obvious the present invention as claimed.

Claim 9 depends indirectly from allowable Claim 1. Van Oorschot and Matyas,
5 taken alone or in combination, fail to teach or suggest the step of encrypting a first section of the payload data, while a second section of the payload data remains unencrypted, the step of processing the unencrypted second section for obtaining the information characterizing the unencrypted second section, and the step of linking the payload data key with the obtained information by
10 means of an invertible logic linkage to obtain a basic value, as claimed in Claim 1, as amended.

Klemba does not remedy any of the deficiencies of Van Oorschot and Matyas. Klemba, taken alone or in combination with Van Oorschot and Matyas, fails to
15 teach or suggest the step of encrypting a first section of the payload data, while a second section of the payload data remains unencrypted, the step of processing the unencrypted second section for obtaining the information characterizing the unencrypted second section, and the step of linking the payload data key with the obtained information by means of an invertible logic
20 linkage to obtain a basic value, as claimed in Claim 1, as amended.

Thus, Applicants respectfully submit that Claim 9 is distinguishable over Van Oorschot, Matyas, and Klemba, taken alone or in combination, and should be allowed. As a result, Applicants respectfully request withdrawal of the rejections
25 and allowance of the Claim.

Claim 10 was rejected under 35 USC 103(a) as being unpatentable over Van Oorschot and Matyas and further in view of US Patent No. 6,198,875 to
30 Edenson et al. (hereinafter "Edenson"). Applicants respectfully submit that Van Oorschot, Matyas, and Edenson, taken alone or in combination, fail to teach, suggest or render obvious the present invention as claimed.

- Claim 10 depends indirectly from allowable Claim 1. Van Oorschot and Matyas, taken alone or in combination, fail to teach or suggest the step of encrypting a firsts section of the payload data, while a second section of the payload data remains unencrypted, the step of processing the unencrypted second section
- 5 for obtaining the information characterizing the unencrypted second section, and the step of linking the payload data key with the obtained information by means of an invertible logic linkage to obtain a basic value, as claimed in Claim 1, as amended.
- 10 Edenson does not remedy any of the deficiencies of Van Oorschot and Matyas. Edenson, taken alone or in combination with Van Oorschot and Matyas, fails to teach or suggest the step of encrypting a firsts section of the payload data, while a second section of the payload data remains unencrypted, the step of processing the unencrypted second section for obtaining the information
- 15 characterizing the unencrypted second section, and the step of linking the payload data key with the obtained information by means of an invertible logic linkage to obtain a basic value, as claimed in Claim 1, as amended.
- Thus, Applicants respectfully submit that Claim 10 is distinguishable over Van
- 20 Oorschot, Matyas, and Edenson, taken alone or in combination, and should be allowed. As a result, Applicants respectfully request withdrawal of the rejections and allowance of the Claim.
- 25 Claim 13 was rejected under 35 USC 103(a) as being unpatentable over Van Oorschot and Matyas and further in view of Schneier. Applicants respectfully submit that Van Oorschot, Matyas, and Schneier, taken alone or in combination, fail to teach, suggest or render obvious the present invention as claimed.
- 30 Claim 13 depends indirectly from allowable Claim 1. Van Oorschot and Matyas, taken alone or in combination, fail to teach or suggest the step of encrypting a firsts section of the payload data, while a second section of the payload data remains unencrypted, the step of processing the unencrypted second section

for obtaining the information characterizing the unencrypted second section, and the step of linking the payload data key with the obtained information by means of an invertible logic linkage to obtain a basic value, as claimed in Claim 1, as amended.

5

Schneier does not remedy any of the deficiencies of Van Oorschot and Matyas. Schneier, taken alone or in combination with Van Oorschot and Matyas, fails to teach or suggest the step of encrypting a first section of the payload data, while a second section of the payload data remains unencrypted, the step of processing the unencrypted second section for obtaining the information characterizing the unencrypted second section, and the step of linking the payload data key with the obtained information by means of an invertible logic linkage to obtain a basic value, as claimed in Claim 1, as amended.

10

Thus, Applicants respectfully submit that Claim 9 is distinguishable over Van Oorschot, Matyas, and Schneier, taken alone or in combination, and should be allowed. As a result, Applicants respectfully request withdrawal of the rejections and allowance of the Claim.

20

Claim 15 was rejected under 35 USC 103(a) as being unpatentable over Van Oorschot in view of US Patent No. 4,899,333 to Roediger (hereinafter "Roediger"). Applicants respectfully submit that Van Oorschot and Roediger, taken alone or in combination, fail to teach, suggest or render obvious the present invention as claimed.

25

Claim 15 depends directly from allowable Claim 1. Van Oorschot fails to teach or suggest the step of encrypting a first section of the payload data, while a second section of the payload data remains unencrypted, the step of processing the unencrypted second section for obtaining the information characterizing the unencrypted second section, and the step of linking the payload data key with the obtained information by means of an invertible logic linkage to obtain a basic value, as claimed in Claim 1, as amended.

30

Roediger does not remedy any of the deficiencies of Van Oorschot. Roediger, taken alone or in combination with Van Oorschot, fails to teach or suggest the step of encrypting a first section of the payload data, while a second section of the payload data remains unencrypted, the step of processing the unencrypted second section for obtaining the information characterizing the unencrypted second section, and the step of linking the payload data key with the obtained information by means of an invertible logic linkage to obtain a basic value, as claimed in Claim 1, as amended.

Thus, Applicants respectfully submit that Claim 15 is distinguishable over Van Oorschot and Roediger, taken alone or in combination, and should be allowed. As a result, Applicants respectfully request withdrawal of the rejections and allowance of the Claim.

Claim 22 was rejected under 35 USC 103(a) as being unpatentable over Van Oorschot in view of Schneier. Applicants respectfully submit that Van Oorschot and Schneier, taken alone or in combination, fail to teach, suggest or render obvious the present invention as claimed.

Claim 22 depends directly from allowable Claim 17. Van Oorschot fails to teach or suggest a method for decrypting an encrypted payload data stream comprising a header and a payload data block containing a first section having encrypted payload data and a second section having unencrypted payload data, the method comprising, *inter alia*, the step of processing the unencrypted second section of said payload data using the processing method used when encrypting to deduce information characterizing the unencrypted second section, as claimed in Claim 17, as amended.

Schneier does not remedy any of the deficiencies of Van Oorschot. Schneier, taken alone or in combination with Van Oorschot, fails to teach or suggest fails to teach or suggest a method for decrypting an encrypted payload data stream

comprising a header and a payload data block containing a first section having encrypted payload data and a second section having unencrypted payload data, the method comprising, *inter alia*, the step of processing the unencrypted second section of said payload data using the processing method used when
5 encrypting to deduce information characterizing the unencrypted second section, as claimed in Claim 17, as amended.

Thus, Applicants respectfully submit that Claim 22 is distinguishable over Van Oorschot and Schneler, taken alone or in combination, and should be allowed.
10 As a result, Applicants respectfully request withdrawal of the rejections and allowance of the Claim.

Claims 29 and 31 were rejected under 35 USC 103(a) as being unpatentable
15 over Van Oorschot in view of US Patent No. 5,315,635 to Kane (hereinafter "Kane"). Applicants respectfully submit that Van Oorschot and Kane, taken alone or in combination, fail to teach, suggest or render obvious the present invention as claimed. Applicants respectfully point out that the present application, as preliminarily amended, has 30 claims presented for examination.

20 Independent Claim 29, as amended, recites a device for decrypting an encrypted payload data stream comprising a header and a payload data block containing a first section having encrypted payload data and a second section having unencrypted payload data, the device comprising, *inter alia*, a processor
25 for processing the unencrypted second section of said payload data using the processing method used when encrypting to deduce information characterizing the unencrypted second section. Van Oorschot fails to teach or suggest a device for decrypting an encrypted payload data stream comprising a header and a payload data block containing a first section having encrypted payload
30 data and a second section having unencrypted payload data, the device comprising, *inter alia*, a processor for processing the unencrypted second section of said payload data using the processing method used when

encrypting to deduce information characterizing the unencrypted second section, as claimed in Claim 29, as amended.

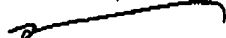
5 Kane does not remedy any of the deficiencies of Van Oorschot. Kane, taken alone or in combination with Van Oorschot, fails to teach or suggest a device for decrypting an encrypted payload data stream comprising a header and a payload data block containing a first section having encrypted payload data and a second section having unencrypted payload data, the device comprising, *inter alia*, a processor for processing the unencrypted second section of said payload
10 data using the processing method used when encrypting to deduce information characterizing the unencrypted second section, as claimed in Claim 29, as amended.

15 Thus, Applicants respectfully submit that Claim 29 is distinguishable over Van Oorschot and Kane, taken alone or in combination, and should be allowed. As a result, Applicants respectfully request withdrawal of the rejections and allowance of the Claim.

CONCLUSION

20 Based on the foregoing, Applicants consider the claimed invention to be distinguished from the art of record. Accordingly, Applicant earnestly solicits the Examiner's withdrawal of the rejections raised in the above referenced Office Action, such that a Notice of Allowance is forwarded to Applicants, and the
25 present application is therefore allowed to issue as a United States Patent.

Respectfully Submitted,



Michael A. Glenn

Reg. No. 30,176

30 Customer No. 22862